Vendor: Microsoft

Exam Code:MS-101

Exam Name: Microsoft 365 Mobility and Security

Version: Demo

QUESTION 1

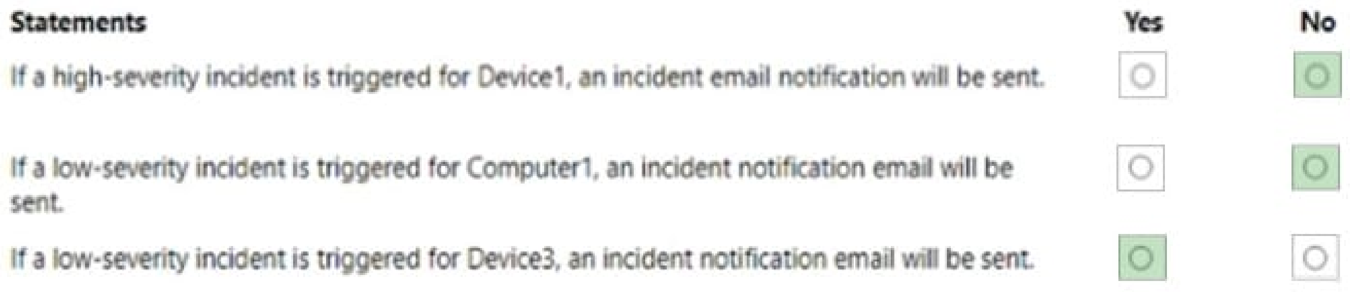
HOTSPOT

You need to meet the technical requirements and planned changes for Intune.

What should you do? To answer, select the appropriate options in the answer area.

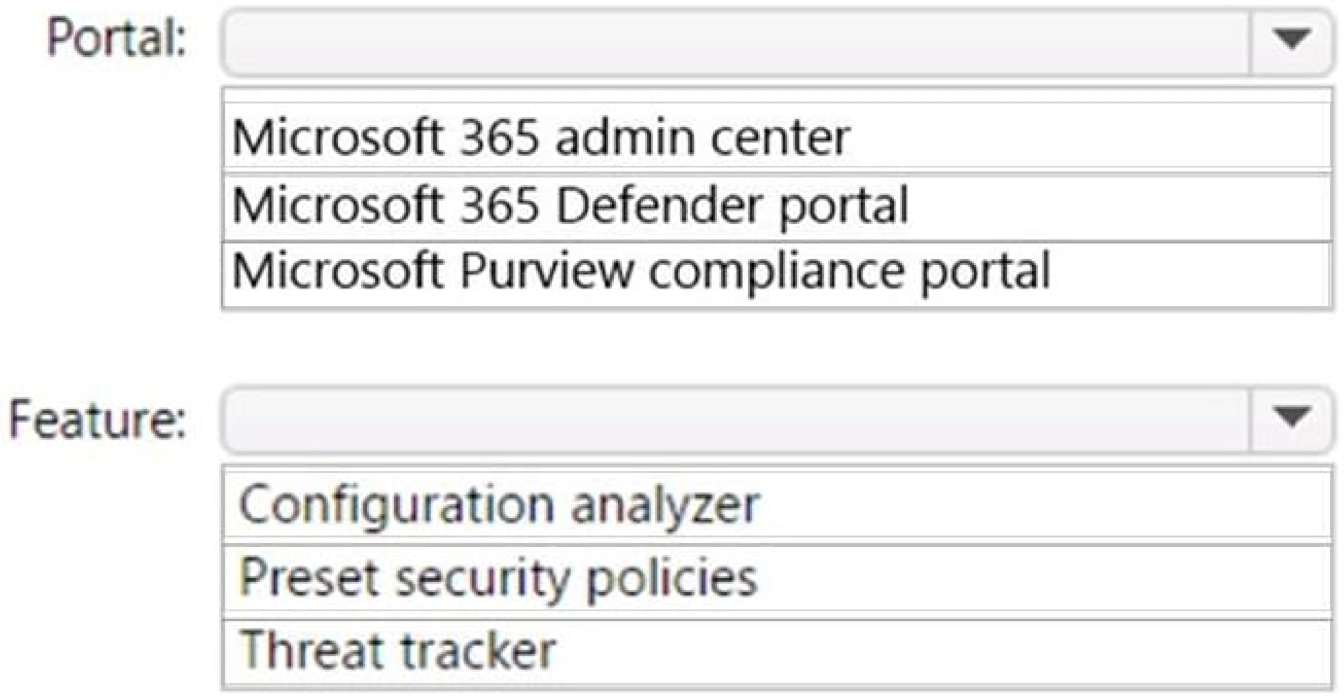
NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
If a high-severity incident is triggered for Device1, an incident email notification will be sent.	○	●
If a low-severity incident is triggered for Computer1, an incident notification email will be sent.	○	●
If a low-severity incident is triggered for Device3, an incident notification email will be sent.	●	○

Correct Answer:



Portal:

Microsoft 365 admin center

Microsoft 365 Defender portal

Microsoft Purview compliance portal

Feature:

Configuration analyzer

Preset security policies

Threat tracker

Reference: https://docs.microsoft.com/en-us/intune/windows-enroll

---

QUESTION 2

You have a Microsoft 365 subscription that uses a default domain named contoso.com.

You have two users named User1 and User2.

From the Security and Compliance admin center, you add User1 to the eDiscovery Manager role group.

From the Security and Compliance admin center, User1 creates a case named Case1.

You need to ensure that User1 can add User2 as a case member. The solution must use the principle of least privilege.

To which role group should you add User2?

A. eDiscovery Manager

B. eDiscovery Administrator

C. Security Administrator

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/add-or-remove-members-from-a-case-in-advanced-ediscovery?view=o365-worldwide

---

QUESTION 3

You need to consider the underlined segment to establish whether it is accurate.

Your company has a Microsoft Azure Active Directory (Azure AD) tenant that includes a Microsoft 365 subscription.

to make sure that administrators have the ability to manage the configuration settings for all the Windows 10 devices, you should configure the Enrollment restrictions settings.

Select "No adjustment required" if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.

What should you configure?

A. No adjustment required.

B. MDM authority

C. MAM authority

D. device enrollment settings

Correct Answer: B

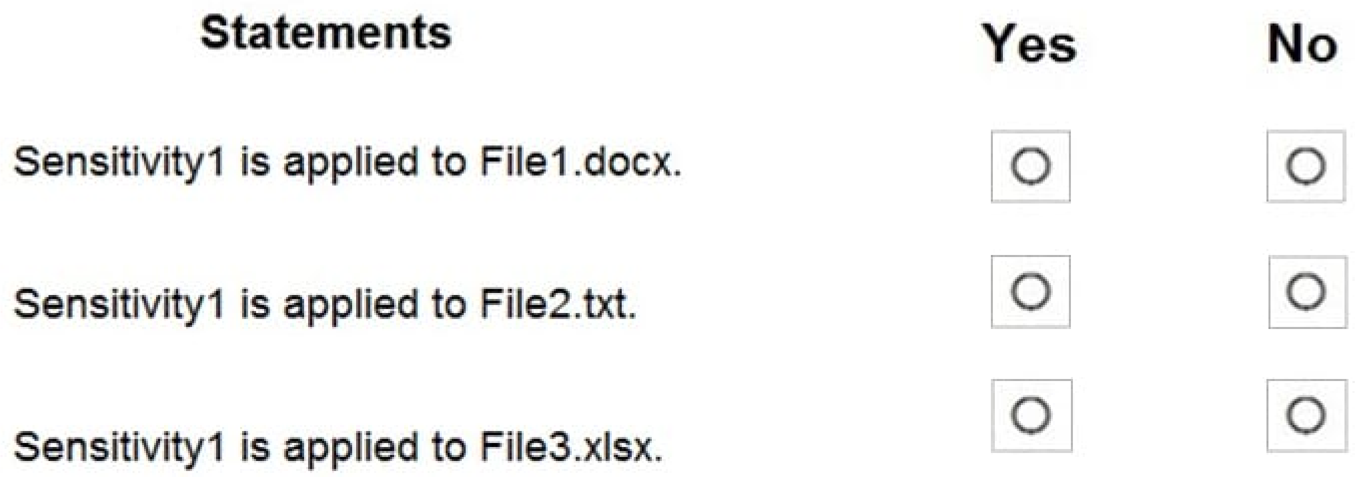
References: https://docs.microsoft.com/en-us/intune/mdm-authority-set

---

QUESTION 4

HOTSPOT

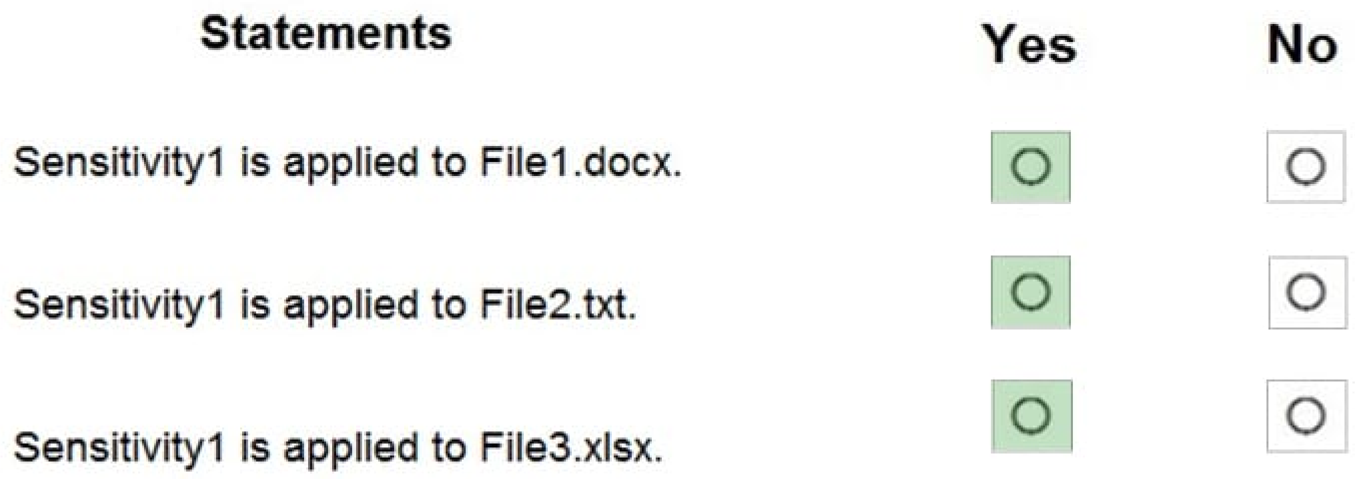
You have a Microsoft 365 ES subscription that has three auto retention policies as show in the following exhibit.



Statements	Yes	No
Sensitivity1 is applied to File1.docx.	○	○
Sensitivity1 is applied to File2.txt.	○	○
Sensitivity1 is applied to File3.xlsx.	○	○

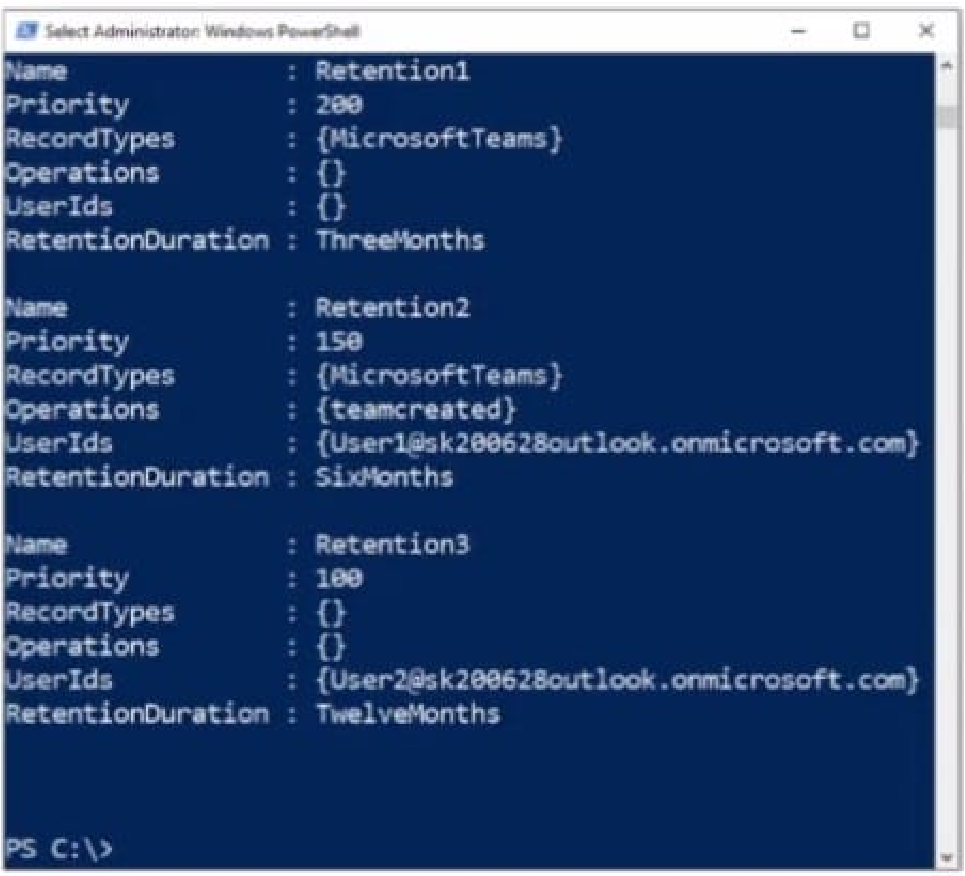
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic NOTE Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
Sensitivity1 is applied to File1.docx.	[✓ ○]	○
Sensitivity1 is applied to File2.txt.	[✓ ○]	○
Sensitivity1 is applied to File3.xlsx.	[✓ ○]	○

Correct Answer:



```
Name              : Retention1
Priority          : 200
RecordTypes       : {MicrosoftTeams}
Operations        : {}
UserIds           : {}
RetentionDuration : ThreeMonths

Name              : Retention2
Priority          : 150
RecordTypes       : {MicrosoftTeams}
Operations        : {teamcreated}
UserIds           : {User1@sk200628outlook.onmicrosoft.com}
RetentionDuration : SixMonths

Name              : Retention3
Priority          : 100
RecordTypes       : {}
Operations        : {}
UserIds           : {User2@sk200628outlook.onmicrosoft.com}
RetentionDuration : TwelveMonths



PS C:\>
```

QUESTION 5

You have a Microsoft 365 subscription.

You plan to enable Microsoft Azure Information Protection.

You need to ensure that only the members of a group named PilotUsers can protect content.

What should you do?

A. Run the Add-AadrmRoleBasedAdministrator cmdlet.

B. Create an Azure Information Protection policy.

C. Configure the protection activation status for Azure Information Protection.

D. Run the Set-AadrmOnboardingControlPolicy cmdlet.

Correct Answer: D

Reference: https://blogs.technet.microsoft.com/kemckinn/2018/05/17/creating-labels-for-azure-information-protection/

QUESTION 6

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).

You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).

You configure pilot co-management.

You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.

You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.

Solution: You create a device configuration profile from the Device Management admin center.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

It looks like the given answer is correct. There is an on-premises Active Directory synced to Azure Active Directory (Azure AD) So the co-management path 1 - Auto-enroll existing clients 1. Hybrid Azure AD

2.

Client agent setting for hybrid Azure ADjoin

3.

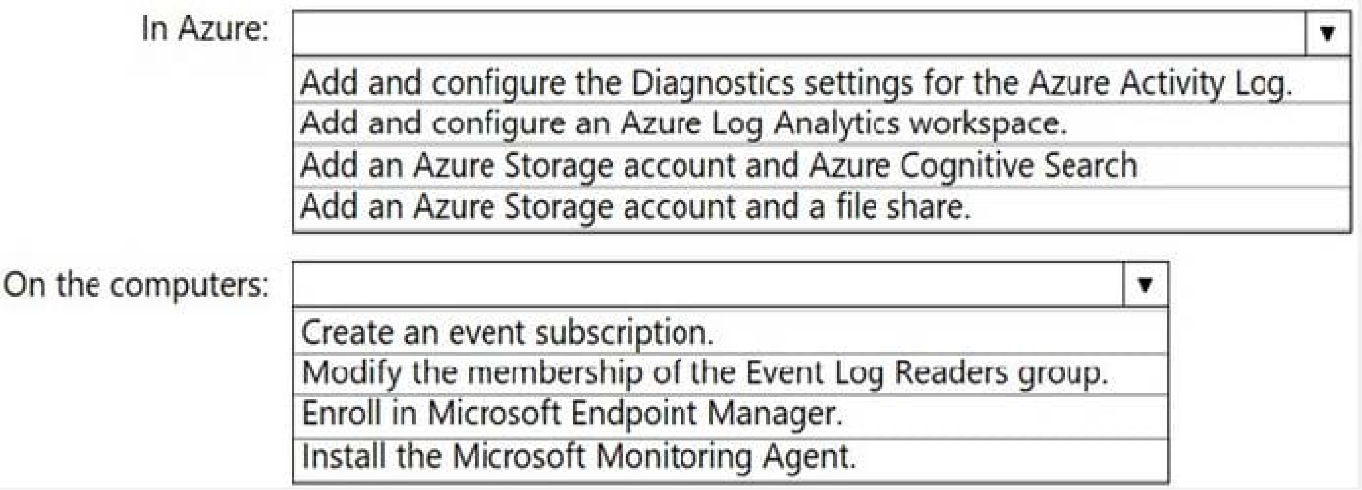
Configure auto-enrollment of devices to Intune 4. Enable co-management in Configuration Manager https://docs.microsoft.com/enus/mem/configmgr/comanage/tutorial-co-manage-client

---

QUESTION 7

HOTSPOT

Your company has a Microsoft 36S subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com. The company stores 2 TBs of data in SharePoint Online document libraries.



In Azure: ▼

- Add and configure the Diagnostics settings for the Azure Activity Log.
- Add and configure an Azure Log Analytics workspace.
- Add an Azure Storage account and Azure Cognitive Search
- Add an Azure Storage account and a file share.

On the computers: ▼

- Create an event subscription.
- Modify the membership of the Event Log Readers group.
- Enroll in Microsoft Endpoint Manager.
- Install the Microsoft Monitoring Agent.

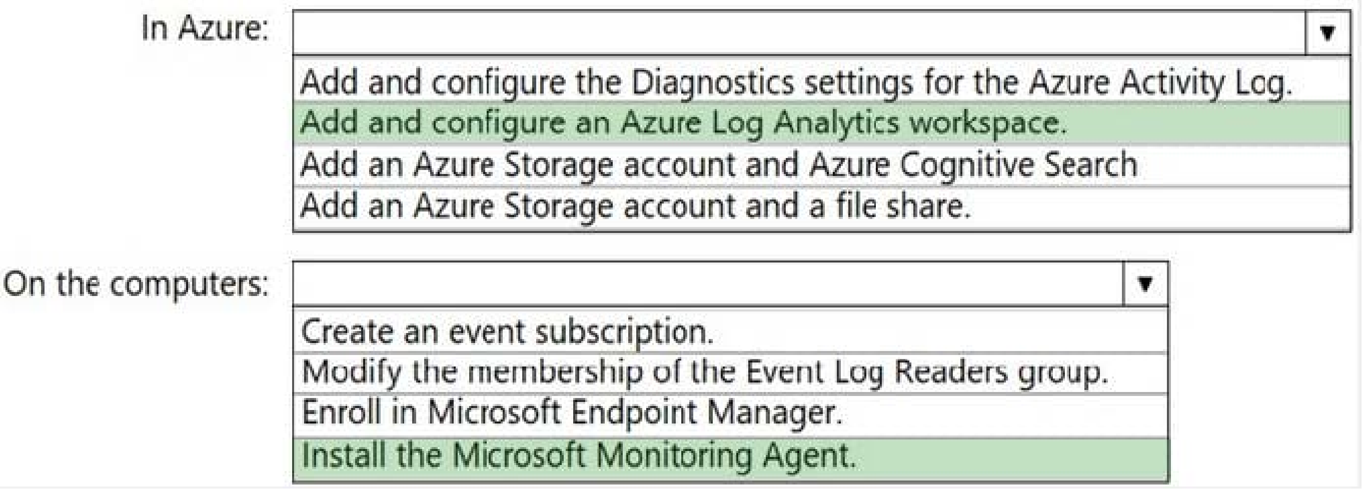
The tenant has the labels shown in the following table.

From the Azure portal, you active unified labeling.

For each of the following statements, select yes if the statement is true Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:



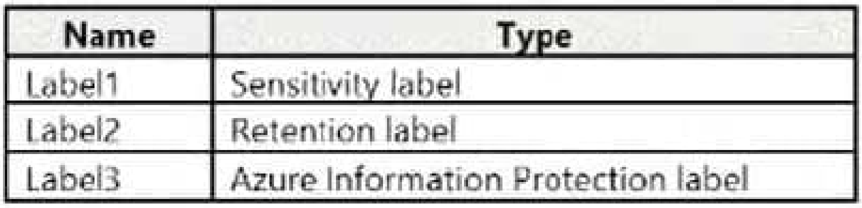
In Azure: ▼

- Add and configure the Diagnostics settings for the Azure Activity Log.
- [✓ Add and configure an Azure Log Analytics workspace.]
- Add an Azure Storage account and Azure Cognitive Search
- Add an Azure Storage account and a file share.

On the computers: ▼

- Create an event subscription.
- Modify the membership of the Event Log Readers group.
- Enroll in Microsoft Endpoint Manager.
- [✓ Install the Microsoft Monitoring Agent.]

Correct Answer:



Name	Type
Label1	Sensitivity label
Label2	Retention label
Label3	Azure Information Protection label

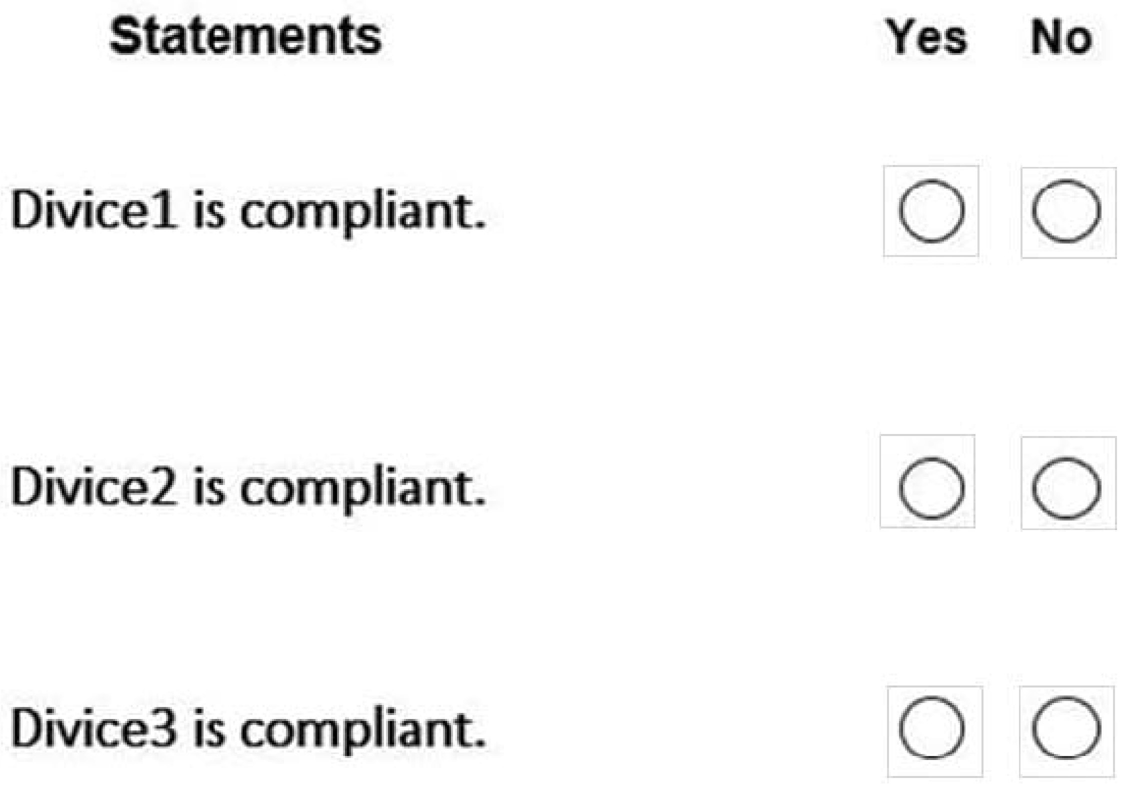
QUESTION 8

HOTSPOT

Your company is based in the United Kingdom (UK).

Users frequently handle data that contains Personally Identifiable Information (PII).

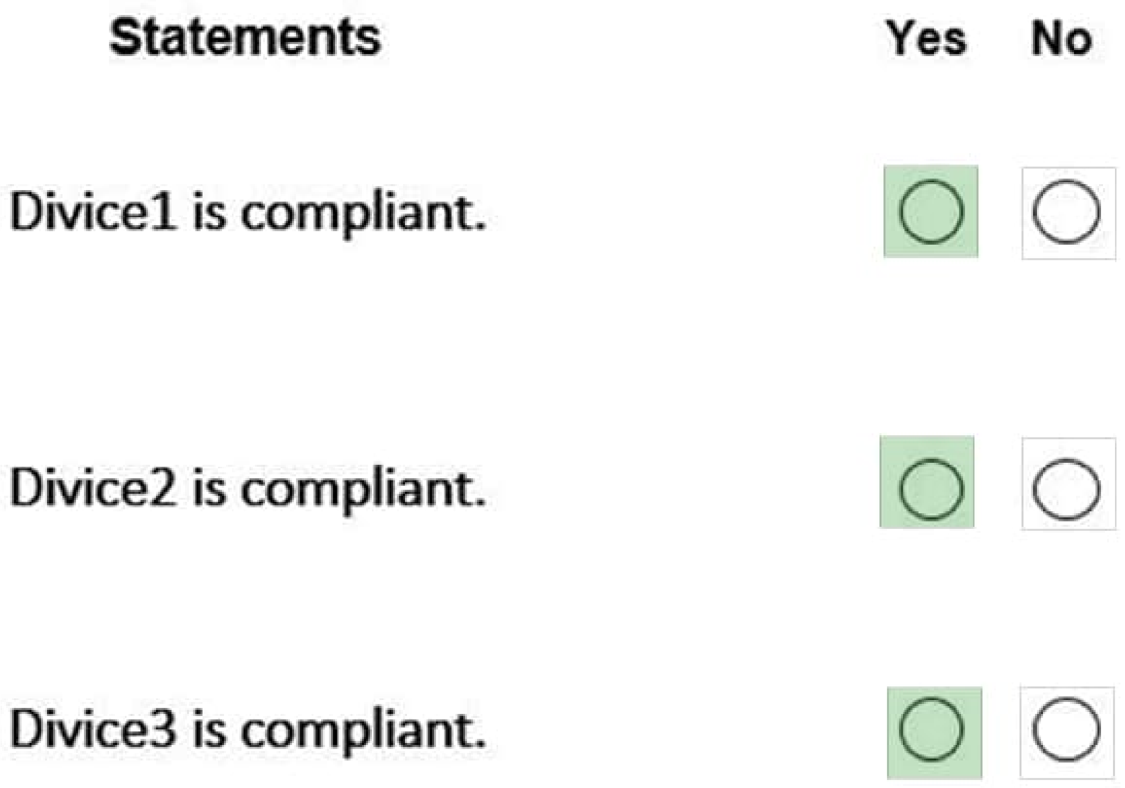
You create a data loss prevention (DLP) policy that applies to users inside and outside the company. The policy is configured as shown in the following exhibit.



Statements	Yes	No
Divice1 is compliant.	○	○
Divice2 is compliant.	○	○
Divice3 is compliant.	○	○

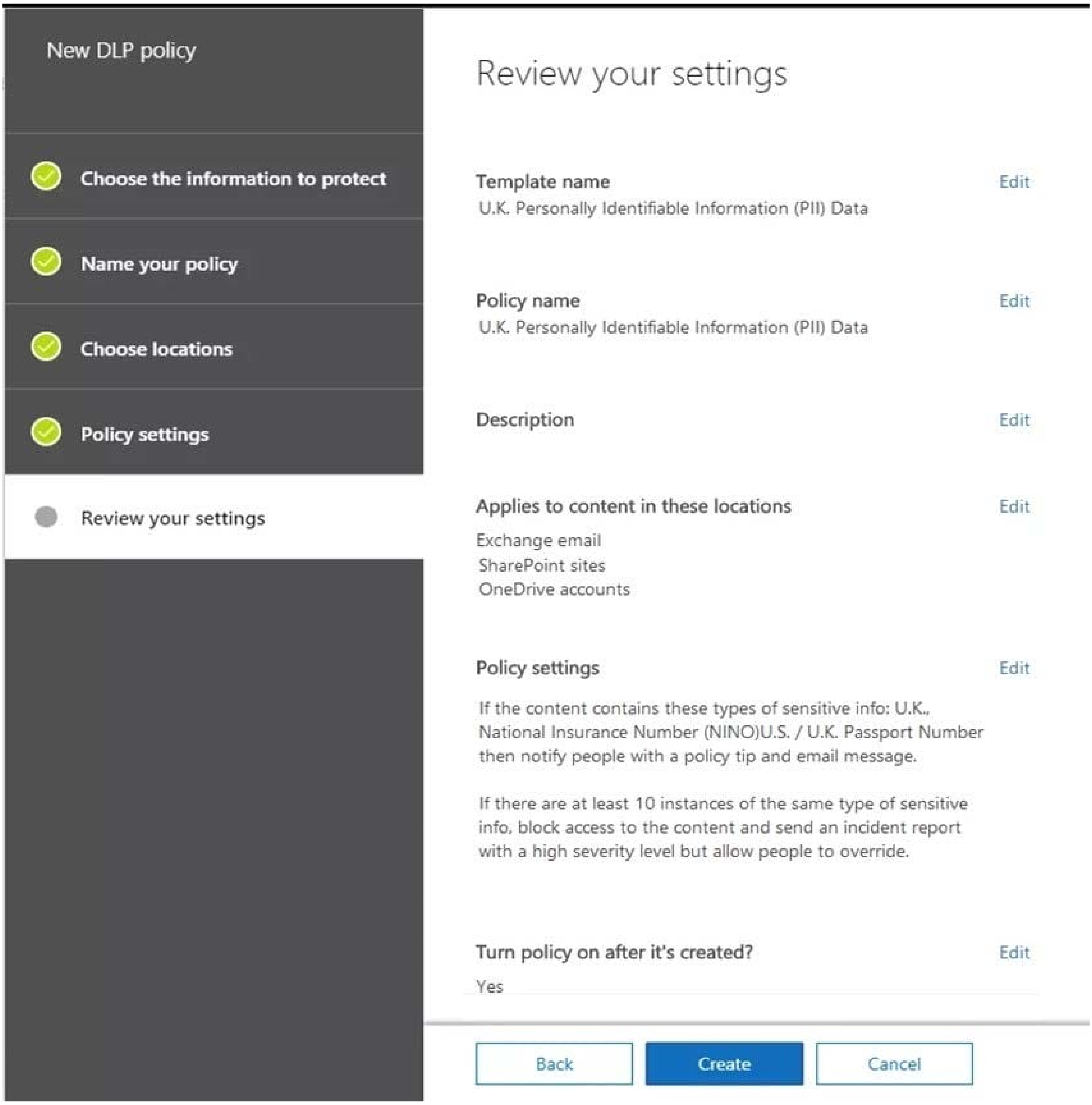
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
Divice1 is compliant.	[✓ ○]	○
Divice2 is compliant.	[✓ ○]	○
Divice3 is compliant.	[✓ ○]	○

Correct Answer:



New DLP policy

✓ Choose the information to protect

✓ Name your policy

✓ Choose locations

✓ Policy settings

● Review your settings

Review your settings

Template name
U.K. Personally Identifiable Information (PII) Data
Edit

Policy name
U.K. Personally Identifiable Information (PII) Data
Edit

Description
Edit

Applies to content in these locations
Exchange email
SharePoint sites
OneDrive accounts
Edit

Policy settings
Edit

If the content contains these types of sensitive info: U.K., National Insurance Number (NINO)U.S. / U.K. Passport Number then notify people with a policy tip and email message.

If there are at least 10 instances of the same type of sensitive info, block access to the content and send an incident report with a high severity level but allow people to override.

Turn policy on after it's created?
Yes
Edit

Allowed blocked, but the user can override the policy

1.

If a user attempts to upload a document to a Microsoft SharePoint site, and the document contains one UK passport number, the document will be: allowed Explanation:

When setting the policy tips and notifications, the document won\\'t be blocked, it just shows a policy tip, if you set up this policy yourself, you will see there are no (block) actions configured for this rule.

2.

If a user attempts to email 100 UK passport numbers to a user in the same company, the email message will be:

blocked, but the user can override the policy https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies

---

QUESTION 9

Your company has five security information and event management (SIEM) appliances. The traffic logs from each appliance are saved to a file share named Logs.

You need to analyze the traffic logs.

What should you do from Microsoft Cloud App Security?

A. Click Investigate, and then click Activity log.

B. Click Control, and then click Policies. Create a file policy.

C. Click Discover, and then click Create snapshot report.

D. Click Investigate, and then click Files.

Correct Answer: C

References: https://docs.microsoft.com/en-us/office365/securitycompliance/investigate-an-activity-in-office-365-cas

---

QUESTION 10

You have a Microsoft 365 E5 subscription.

You need to identify which users accessed Microsoft Office 365 from anonymous IP addresses during the last seven days.

What should you do?

A. From the Cloud App Security admin center, select Users and accounts.

B. From the Microsoft 365 security center, view the Threat tracker.

C. From the Microsoft 365 admin center, view the Security and compliance report.

D. From the Azure Active Directory admin center, view the Risky sign-ins report.

Correct Answer: A

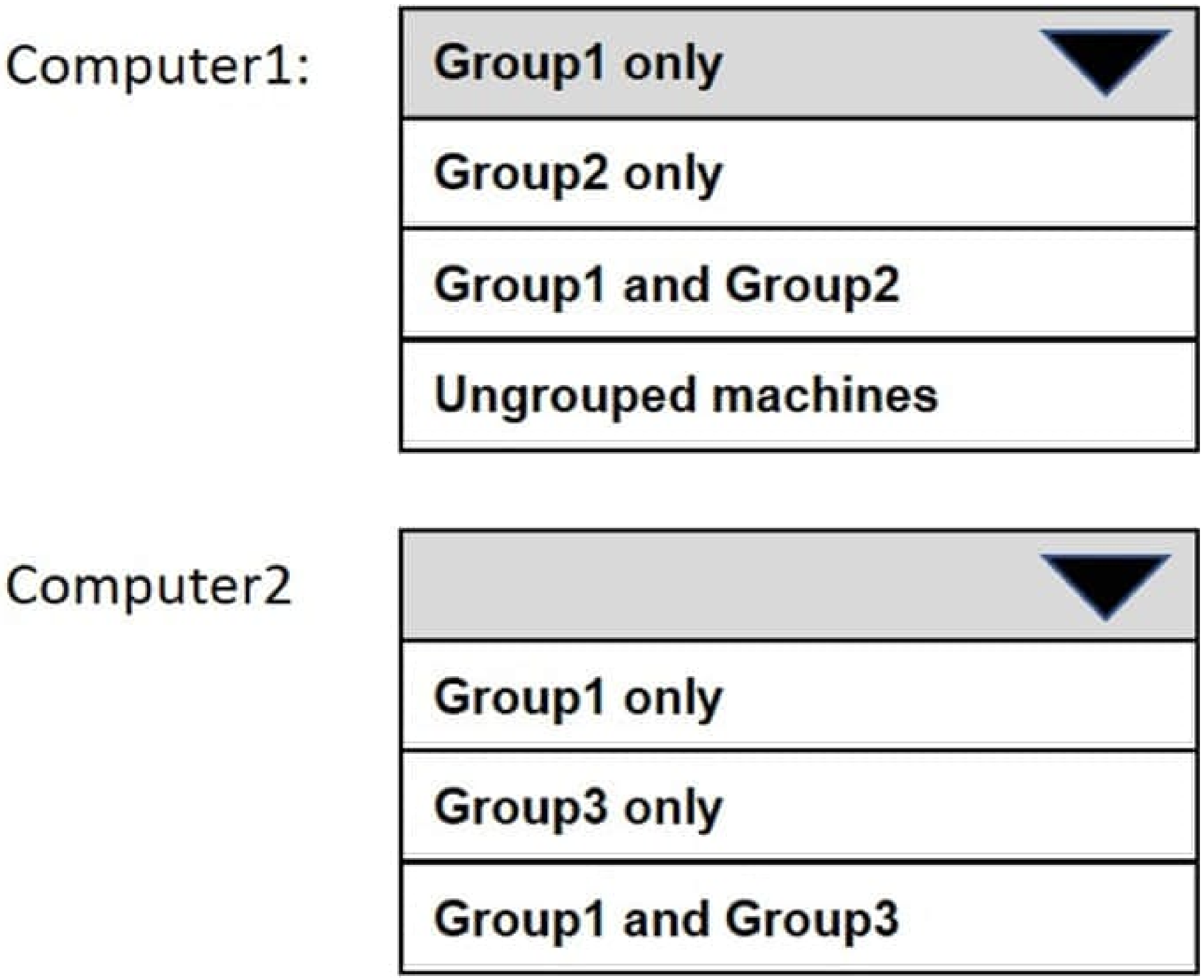
QUESTION 11

HOTSPOT

You have a Microsoft 365 subscription.

You are configuring permissions for Security and Compliance.

You need to ensure that the users can perform the tasks shown in the following table.

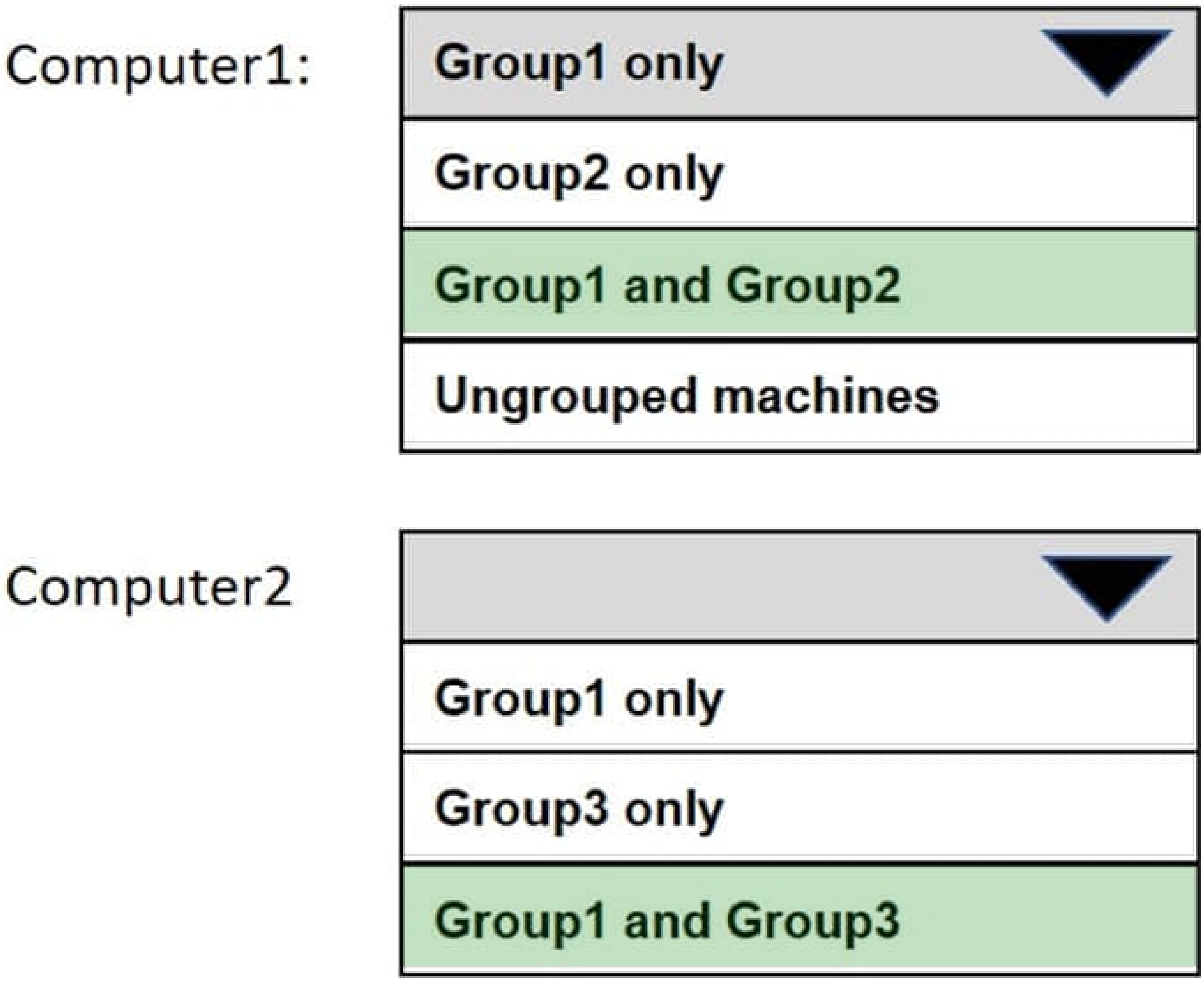


The solution must use the principle of least privilege.

To which role should you assign each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Computer1:

Group1 only

Group2 only

[✓ Group1 and Group2]

Ungrouped machines

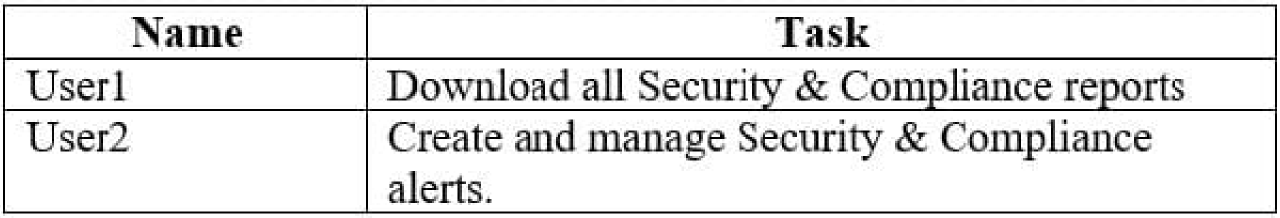
Computer2

Group1 only

Group3 only

[✓ Group1 and Group3]

Correct Answer:



Name	Task
User1	Download all Security & Compliance reports
User2	Create and manage Security & Compliance alerts.

References: https://docs.microsoft.com/en-us/office365/securitycompliance/permissions-in-the-security-and-compliance-center#mapping-of-role-groups-to-assigned-roles

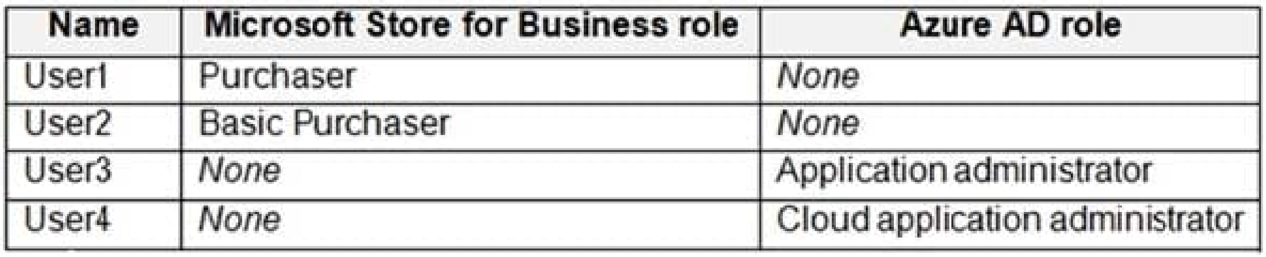
---

QUESTION 12

Your company has a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You sign up for Microsoft Store for Business.

The tenant contains the users shown in the following table.



Name	Microsoft Store for Business role	Azure AD role
User1	Purchaser	*None*
User2	Basic Purchaser	*None*
User3	*None*	Application administrator
User4	*None*	Cloud application administrator

Microsoft Store for Business has the following Shopping behavior settings:

1.

Make everyone a Basic Purchaser is set to Off.

2.

Allow app requests is set to On.

You need to identify which users can add apps to the Microsoft Store for Business private store.

Which users should you identify?

A. User1 and User2 only

B. User3 only

C. User1 only

D. User3 and User4 only

Correct Answer: A